REMARKS

In the final Office Action, the Examiner

- rejects claims 1-7, 10, 12-18, 21, 23-25, 27, 31-33, 35, 37, 38, 40, and 41 under 35 U.S.C. § 103(a) as allegedly unpatentable over GLEICHAUF et al. (U.S. Patent No. 6,499,107, hereinafter GLEICHAUF), GLEICHAUF et al. (U.S. Patent No. 6,324,656; hereinafter GLEICHAUF 2), NIKANDER et al. (U.S. Patent No. 6,253,321; hereinafter NIKANDER), COPELAND, III (U.S. Patent Application Publication No. 2003/0105976; hereinafter COPELAND), and ALEXANDER et al. (U.S. Patent Application Publication No. 2004/0258073; hereinafter ALEXANDER);
- rejects claims 22 and 39 under 35 U.S.C. § 103(a) as allegedly unpatentable over GLEICHAUF, GLEICHAUF 2, and NIKANDER; and
- rejects claims 42-46, 49, 50, and 52-69 under 35 U.S.C. § 103(a) as allegedly unpatentable over GLEICHAUF, NIKANDER, TRCKA et al (U.S. Patent No. 6,453,345; hereinafter TRCKA), COPELAND, and ALEXANDER.

Applicants respectfully traverse these rejections.

By way of the present amendment, Applicants cancel claims 14, 22, 33, 35, 39, 46, 49, 50, 52-54, 59, 64, and 67-69 without prejudice or disclaimer and amend claims 1-7, 10, 12, 13, 15-18, 21, 23-25, 27, 31, 32, 37, 38, 40-45, 55-58, and 60-66 to improve form. No new matter has been

added by way of the present amendment. Claims 1-7, 10, 12, 13, 15-18, 21, 23-25, 27, 31, 32, 37, 38, 40-45, 55-58, and 60-66 are pending.

Rejection under 35 U.S.C. § 103(a) based on GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER

Pending claims 1-7, 10, 12, 13, 15-18, 21, 23-25, 27, 31, 32, 37, 38, 40 and 41 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over GLEICHAUF, GLEICHAUF #2, NIKANDER, COPELAND, and ALEXANDER. Applicants respectfully traverse this rejection.

Amended independent claim 1 recites a method, comprising reassembling a plurality of TCP packets, in network traffic, into a TCP stream; inspecting the TCP stream to detect information indicative of a security breach; grouping the plurality of TCP packets into packet flows and communication sessions; storing information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptors; dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of the security breach; forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the security breach, where inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database, querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the

protocol database, and searching for a network attack identifier, in the TCP stream, based on the packet flow descriptors and communication sessions associated with the TCP stream. GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER, whether taken alone or in any reasonable combination, do not disclose or suggest one or more features of amended claim 1.

For example, GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER do not disclose or suggest storing information regarding packet flows in packet flow descriptors, where each of the packet flow descriptors points to a communication session and each of the communications sessions points to one or more of the packet flow descriptors, as recited by amended claim 1. The Examiner concedes that GLEICHAUF, GLEICHAUF 2, and NIKANDER do not disclose "grouping the plurality of TCP packets into packet flows and sessions; storing the packet flows in packet flow descriptors and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream," and relies on ¶ 0050 of COPELAND for allegedly disclosing this feature. (Final Office Action, p. 5.) Without acquiescing in the Examiner's allegation regarding previously presented claim 1, Applicants submit that GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER do not disclose or suggest the above-identified feature of amended claim 1.

Paragraph 0050 of COPELAND discloses:

> In accordance with an aspect of the invention, the intrusion detection engine 155 works by assigning data packets 101 to various flows. The engine 155 collects information about and statistics associated with each flow and stores this information and statistics in a database 160.

> The flow database 160 comprises a flow data structure 162 and a host data structure 166. The flow data structure 162 stores collected flow information such as the IP addresses. The engine determines which host has a lower IP address and assigns that host IP0. The other host is assigned IP1. Port0 is associated with IPO and port1 is the service connection port for host1. The flow data structure 162 also stores time and other related packet information derived from the packet header. In the disclosed embodiment, this time information (e.g. time of the first packet, time of the last packet) is utilized to measure the elapse of time for purposes of flow delimiting, as described above.

This paragraph of COPELAND discloses that an intrusion detection engine collects information about and statistics associated with each flow and stores this information and statistics in a database. The database includes a flow data structure 162 that stores collected flow information, such as IP addresses, time, and other related packet information derived from a packet header. This paragraph of COPELAND does not disclose or suggest storing information regarding packet flows in packet flow descriptors, where each of the packet flow descriptors points to a communication session and each of the communications sessions points to one or more of the packet flow descriptors, as recited by amended claim 1. In fact, neither this paragraph, nor any other paragraph of COPELAND even mentions that a packet flow descriptor points to a communication session, or that each communication session points to one or more packet flow descriptors.

Rather, COPELAND merely discloses reading and writing to a flow data structure 162 to identify possible intruders. (See, e.g., ¶ 0105 of COPELAND.) Applicants submit that merely reading and writing to a flow data structure cannot reasonably be construed to correspond to storing information regarding packet flows in packet flow descriptors, where each of the packet flow descriptors points to a communication session and each of

the communication sessions points to one or more of the packet flow descriptors, as recited by amended claim 1.

Applicants submit that the disclosure of ALEXANDER does not cure the deficiencies in the disclosures of GLEICHAUF, GLEICHAUF 2, NIKANDER, and COPELAND, as set forth above.

For at least the foregoing reasons, Applicants submit that amended claim 1 is patentable over GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER, whether taken alone or in any reasonable combination. Accordingly, Applicants request that the Examiner reconsider and withdraw the rejection of amended claim 1 under 35 U.S.C. § 103(a) based on GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER.

Claims 2-7, 10, 12, 13, 15-17, 21, and 23 depend from claim 1. Therefore, Applicants submit that claims 2-7, 10, 12, 13, 15-17, 21, and 23 are patentable over GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to amended claim 1. Accordingly, Applicants request that the Examiner reconsider and withdraw the rejection of claims 2-7, 10, 12, 13, 15-17, 21, and 23 under 35 U.S.C. § 103(a) based on GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER.

Amended independent claims 18, 24, and 27 recite features similar to (yet possibly of different scope than) features described above with respect to amended claim 1. Therefore, Applicants submit that amended claims 18, 24, and 27 are patentable over GLEICHAUF, GLEICHAUF 2, NIKANDER,

COPELAND, and ALEXANDER, whether taken alone or in any reasonable combination, for at least reasons similar to the reasons given above with respect to amended claim 1. Accordingly, Applicants request that the Examiner reconsider and withdraw the rejection of amended claims 18, 24, and 27 under 35 U.S.C. § 103(a) based on GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER.

Pending claims 25, 31, 37, 38, 40, and 41 depend from claim 24, and claim 32 depends from claim 27. Therefore, Applicants submit that claims 25, 31, 32, 37, 38, 40, and 41 are patentable over GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to amended claims 24 and 27, respectively. Accordingly, Applicants request that the Examiner reconsider and withdraw the rejection of claims 25, 31, 32, 37, 38, 40, and 41 under 35 U.S.C. § 103(a) based on GLEICHAUF, GLEICHAUF 2, NIKANDER, COPELAND, and ALEXANDER.

Rejection under 35 U.S.C. § 103(a) based on GLEICHAUF, GLEICHAUF 2, and NIKANDER

Claims 22 and 39 stand rejected under 35 U.S.C. § 103(a) as unpatentable over GLEICHAUF, GLEICHAUF 2, and NIKANDER. Applicants submit that this rejection is moot in view of the cancelation of these claims.

Rejection under 35 U.S.C. § 103(a) based on GLEICHAUF, NIKANDER, TRCKA, COPELAND, and ALEXANDER

Pending claims 42-45, 55-58, and 60-66 stand rejected under 35 U.S.C. § 103(a) as unpatentable over GLEICHAUF, NIKANDER, TRCKA, COPELAND, and ALEXANDER. Applicants respectfully traverse this rejection.

Amended independent claims 42 and 57 recite features similar to (yet possibly of different scope than) features described above with respect to amended claim 1. Without acquiescing in the rejection of claims 42 and 57, Applicants submit that the disclosure of TRCKA does not cure the deficiencies in the disclosures of GLEICHAUF, NIKANDER, COPELAND, and ALEXANDER, as set forth above with respect to amended claim 1. Therefore, Applicants submit that amended claims 42 and 57 are patentable over GLEICHAUF, NIKANDER, TRCKA, COPELAND, and ALEXANDER, whether taken alone or in any reasonable combination, for at least reasons similar to the reasons given above with respect to amended claim 1. Accordingly, Applicants request that the Examiner reconsider and withdraw the rejection of amended claims 42 and 57 under 35 U.S.C. § 103(a) based on GLEICHAUF, NIKANDER, TRCKA, COPELAND, and ALEXANDER.

Pending claims 43-45, 55, and 56 depend from claim 42, and pending claims 58 and 60-66 depend from claim 57. Therefore, Applicants submit that claims 43-45, 55, 56, 58, and 60-66 are patentable over GLEICHAUF, NIKANDER, TRCKA, COPELAND, and ALEXANDER, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to amended claims 42 and 57, respectively. Accordingly, Applicants

request that the Examiner reconsider and withdraw the rejection of claims 43-45, 55, 56, 58, and 60-66 under 35 U.S.C. § 103(a) based on GLEICHAUF, NIKANDER, TRCKA, COPELAND, and ALEXANDER.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request the Examiner's reconsideration of this application, and the timely allowance of the proposed pending claims.

As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such assertions (e.g., whether a reference constitutes prior art, reasons to modify a reference or to combine references, assertions as to dependent claims, allegations of Official Notice, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY & HARRITY, LLP

By: /Michael S. Brooke, Reg. No. 41,641/
Michael S. Brooke
Registration No. 41,641

Date: June 30, 2011

11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
(571) 432-0800

Customer Number: 44987